日志审计中心产品功能简介

日志审计中心是 SGA 的一套日志审计系统。系统大致分为日志审计、数据报表、系统设置、日志查询和备份恢复共五大模块。

日志审计中心能够统计的内容按表排列如下：

主模块	功能模块	详细描述
日志审计	登录日志审计	基于时间段查询用户（可以为单个用户或者所有用户）的登录次数、用户的总使用时长、用户的平均使用时长。
	资源访问日志审计	基于时间段查询用户（可以为单个用户或者所有用户）对资源（可以选择为所有资源、某类型资源、某个资源）的访问次数，并且以饼状图描述各类资源。
数据报表	用户活跃程度	以用户为单位（并且显示用户姓名和用户所属组），排列出用户的登录 IP、登录的终端类型、登录次数、登录总时长、最后登录时间。并且支持下载为.csv 和.pdf 格式文件。
	资源活跃程度	基于时间段，以具体某资源为单位，排列出资源类型、访问总次数、最后访问时间。
日志查询	系统日志	基于时间段查询用户登录的客户端信息（客户端类型、）和应用使用日志，并且记录传送日志的 SGA 地址。且支持下载为.csv 和.pdf 格式文件。
	用户登录日志	记录每一次的登录或登出的记录，包括时间、用户名、登录 IP、终端类型、硬件特征码、MAC 地址、计算机名、访问时间。且支持下载为.csv 和.pdf 格式文件。
	资源访问日志	详细排列出用户（可以为单个用户或者所有用户）对资源（可以选择为所有资源、某类型资源、某个

		资源）的访问情况。且支持下载为.csv 和.pdf 格式文件。
	文件操作日志	记录对 iBox 文件上传下载操作时的用户名、时间点、文件名（注：目前不会记录禁止上传下载的日志）。且支持下载为.csv 和.pdf 格式文件。

说明：

1. **安装“日志审计中心”时，请确保杀毒软件和 360 卫士/电脑管家类的保护软件都已退出；**
2. **如果 SGA 在外网，请映射日志审计中心服务器的 3306 端口。**
3. **需要安装 NET Frame work 4.0 才能使用**

进入 SGA 后台【日志中心】→【日志服务配置】，勾选『启用远端日志中心服务』，

服务器地址：日志中心服务器的地址，即为安装了【日志审计中心.exe】的服务器。

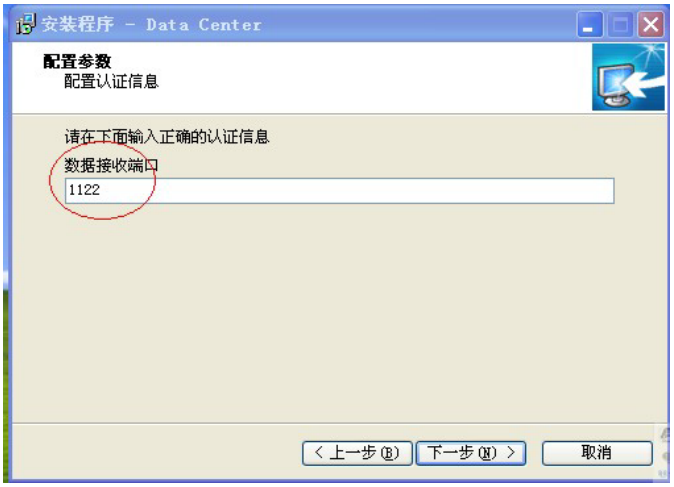
服务器端口：与日志审计中心服务器传送日志的端口，必须保持与服务器上的配置一直

用户名：SGA 与日志审计中心服务器认证的用户

密码：SGA 与日志审计中心服务器认证用户的密码

首先需要准备一台日志审计中心服务器，安装日记审计中心软件， 

安装的时候，一直下一步，在填写端口的时候，请保持与 SGA 后台的【日志中心】→【日志服务器配置】的服务器端口一致。



安装好后，后台访问端口是 7777，本机直接访问 http://127.0.0.1:7777 账号密码 admin/admin。

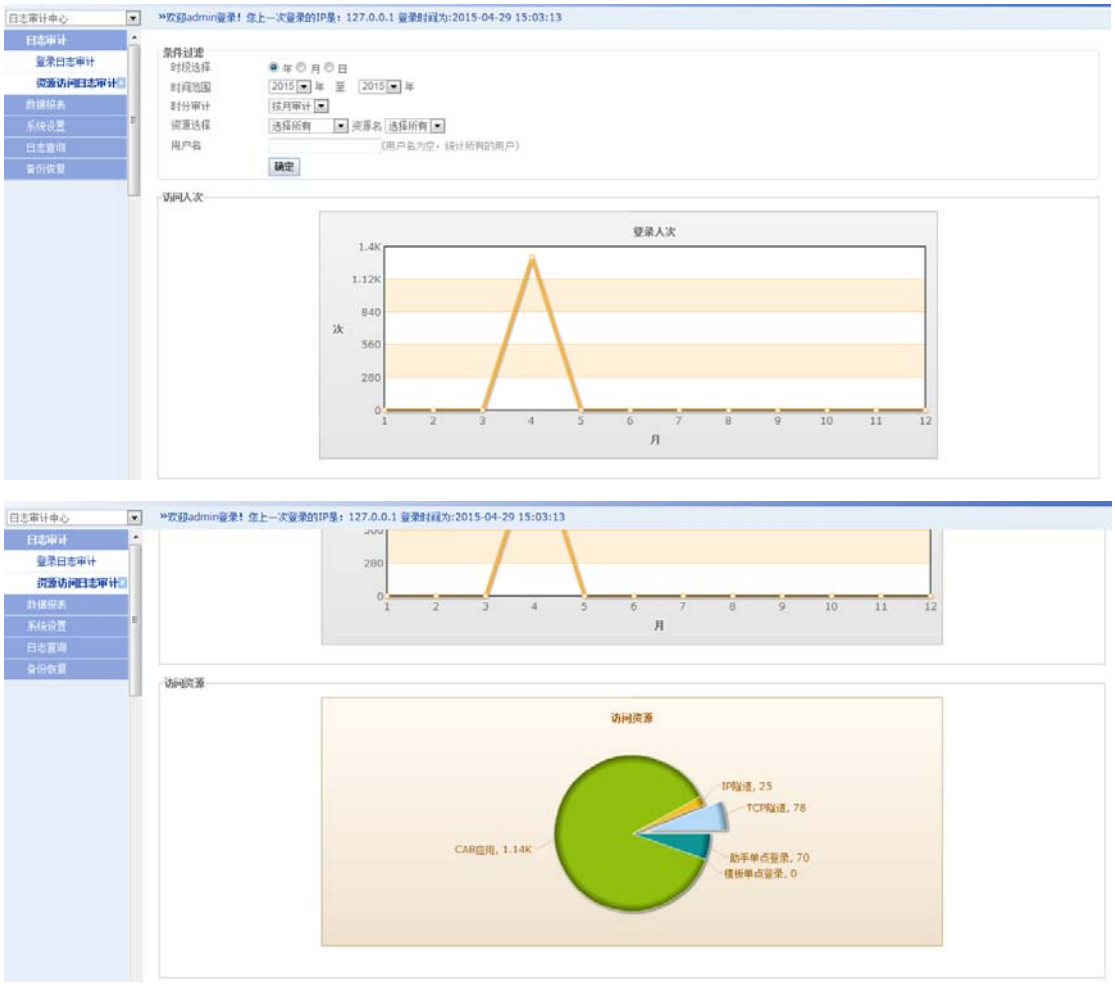
进入日志审计中心后台，【系统设置】→【发送端配置】添加用户，保证与【日志中心】→【日志服务配置】里的用户名密码一致。

1、日志审计

【日志审计】分为【登陆日志审计】和【资源访问日志审计】两大模块。

(1)、【登陆日志审计】基于时间段查询用户（可以为单个用户或者所有用户）的登录次数、用户的总使用时长、用户的平均使用时长。

(2)、【资源访问日志审计】基于时间段查询用户（可以为单个用户或者所有用户）对资源（可以选择为所有资源、某类型资源、某个资源）的访问次数，并且以饼状图描述各类资源。



2、数据报表

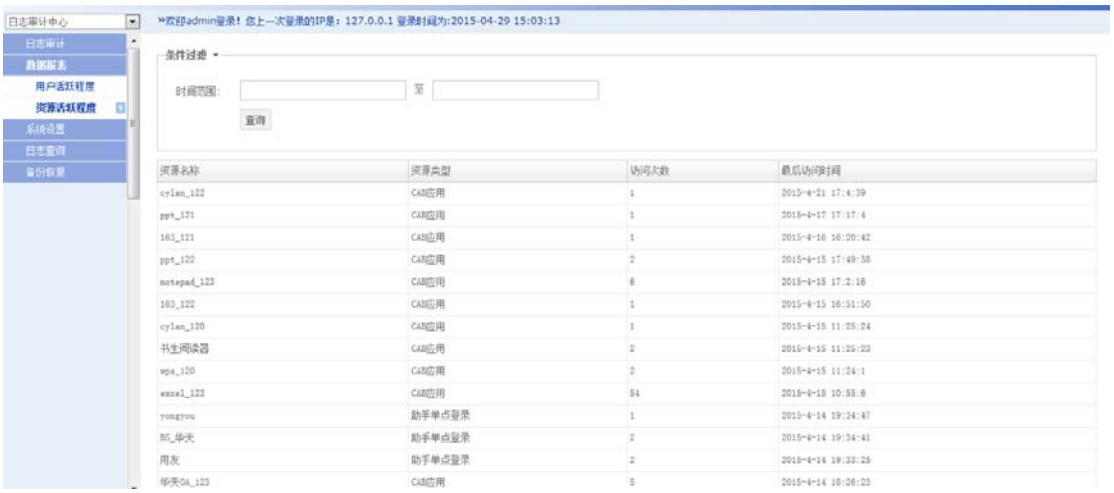
【数据报表】包括【用户活跃程度】和【资源活跃程度】，主要反应了用户活跃程度和资源活跃程度。方便管理员直观了解系统登录情况。并可根据单个用户进行具体查询。

(1)、用户活跃程度

以用户为单位（并且显示用户姓名和用户所属组），排列出用户的登录 IP、登录的终端类型、登录次数、登录总时长、最后登录时间。并且支持下载为.csv 和.pdf 格式文件。

(2)、资源活跃程度

基于时间段，以具体某资源为单位，排列出资源类型、访问总次数、最后访问时间。



3、系统设置

【系统设置】主要分为【用户管理】和【发送端配置】。

(1)、用户管理是给用户分配日志审计中心的管理账号，此账号有管理员账号和一般查看数据用户账户的权限划分。

(2)、发送端配置是建立 SGA 和日志审计中心传输日志的账号。

4、日志查询

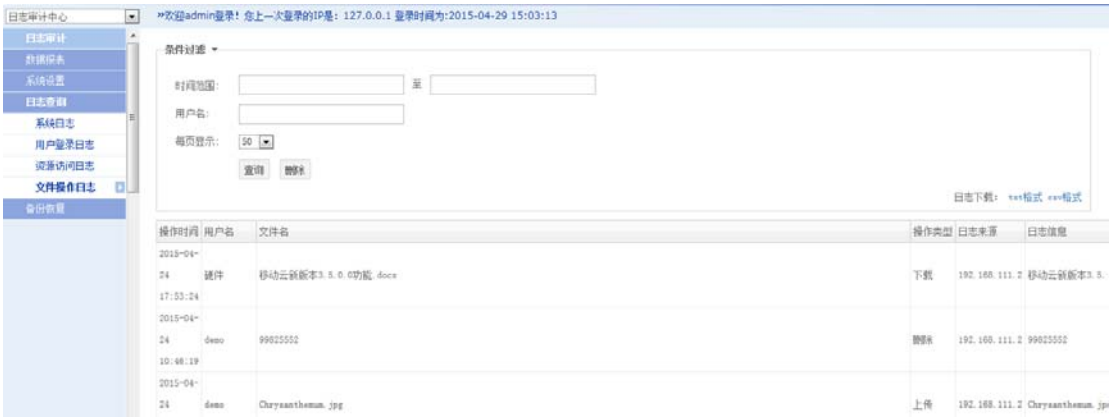
【日志查询】里包括【系统日志】，【用户登录日志】、【资源访问日志】和【文件操作日志】。

(1)、基于时间段查询用户登录的客户端信息（客户端类型、）和应用使用日志，并且记录传送日志的 SGA 地址。且支持下载为.csv 和.pdf 格式文件。

(2)、记录每一次的登录或登出的记录，包括时间、用户名、登录 IP、终端类型、硬件特征码、MAC 地址、计算机名、访问时间。且支持下载为.csv 和.pdf 格式文件。

(3)、详细排列出用户（可以为单个用户或者所有用户）对资源（可以选择为所有资源、某类型资源、某个资源）的访问情况。且支持下载为.csv 和.pdf 格式文件。

（4）、记录对 iBox 文件上传下载操作时的用户名、时间点、文件名（注：目前不会记录禁止上传下载的日志）。且支持下载为.csv 和.pdf 格式文件。



5、备份恢复

可将数据保存，并且上传之前有保存的数据。